REMARKS

In response to the above-identified Office Action, Applicant seeks reconsideration of the application. In this response, no claims have been canceled, no claims have been added, and Claim 1, 2, 8, 11 and 18 have been amended. Accordingly, Claims 1-26 are pending.

I. Claim Objections

In the Office Action, the Examiner objects to the claims for various informalities. This matter is believed to be addressed by the claim amendments submitted herewith. It is there fore respectfully submitted that the objection to the claims be withdrawn.

II. Claims Rejected Under 35 U.S.C. § 112

Claims 1 and 2 are rejected under 35 U.S.C. §112, second paragraph, as being indefinite. Applicant has amended Claims 1 and 2 to clarify that the bus key is derived based on the following: [1] a portion of the key distribution data block, [2] a device key and [3] a nonce. Applicant believes that there is no ambiguity in the amended claims. It is therefore respectfully submitted that the rejection under 35 U.S.C. §112 be withdrawn.

III. Claims Rejected Under 35 U.S.C. § 102

The Examiner rejects Claims 1-4, 6-9, 11-19 and 21-26 under 35 U.S.C. §102(a) as anticipated by Content Protection for Recordable Media Specification Revision 0.94 by IBM et al. (IBM). Applicant respectfully traverses this rejection.

To anticipate a claim, the relied upon reference must disclose every limitation of the claim. Among other limitations, independent Claim 1 recites an encryption subsystem that encrypts data accessed from a storage medium using an encryption bus key prior to transmitting the encrypted data via a data bus. The claimed encryption bus key is derived based on, among other things, the key distribution data block contained in the storage medium and the nonce generated by a number generator. Applicant submits that at least these limitations are not disclosed by IBM.

In rejecting Claim 1, the Examiner asserts that "IBM discloses a system comprising: a number generator to generate a nonce (page 5-5, lines 1-6); and an encryption subsystem to encrypt data accessed from a storage medium containing a key distribution data block using an encryption bus key prior to transmitting the encrypted data via a data bus (page 5-4, lines 1-10),

wherein said encryption bus key is derived based on at least a portion of the key distribution data block, at least one device key assigned to said encryption subsystem and the nonce generated by the number generator (page 5-5, lines 1-16; page 6-3 page 6-4)."

In doing so, it appears that the Examiner may be equating IBM's title key K_t generated by using a random number generator with the claimed encryption bus key. Applicant notes that Claim 1 requires that the claimed encryption bus key is used to encrypt data accessed from a storage medium prior to transmitting the encrypted data via a data bus. Additionally, Claim 1 further requires that the claimed encryption bus key is derived based on [1] a portion of the key distribution data block, [2] a device key assigned to the encryption subsystem and [3] the nonce generated by the number generator, as recited in Claim 1.

However, the title key K_t described by IBM is not used to encrypt data accessed from a storage medium prior to transmitting the encrypted data via a data bus, as set forth in the claimed system. Furthermore, the title key K_t described by IBM is not derived based on [1] a portion of the key distribution data block, [2] a device key assigned to the encryption subsystem and [3] the nonce generated by the number generator, as set forth in the claimed system. Thus, IBM does not disclose an encryption subsystem to encrypt data accessed from a storage medium containing a key distribution data block using an encryption bus key prior to transmitting the encrypted data via a data bus, wherein the encryption bus key is derived based on [1] a portion of the key distribution data block, [2] a device key assigned to said encryption subsystem and [3] the nonce generated by the number generator, as recited in independent Claim 1.

Instead, the title key K_t of IBM is used by a recording device to encrypt data before storing the data on a storage medium. In IBM, the playback device reads the title key from the disc and uses the title key to decrypt the data stored on the storage medium. Such a system may be ineffective in resisting against "replay" attack. In replay attack, an attacker reroutes encrypted data going from a storage device to a host device and records the encrypted data onto a recording medium. Additionally, when the host device access the key distribution data block embedded in the storage medium the attacker also records the key distribution data block onto the same recordable medium. The copy of the key distribution data block and the encrypted data captured at the time of the transmission may be played on a conventional medium player system by presenting the encrypted data to the host device as though it was coming from a legitimate storage device.

Such a problem would not occur with the system claimed in the claims, which uses a nonce value to generate an encryption bus key. Because the nonce value used by the host device to generate its decryption bus key during replay of the enciphered data will be different than the nonce value used by the storage device to generate its encryption bus key at the time of enciphering, this type of replay attack will be prevented. In other words, by using the nonce to generate the bus key, the bus key obtained by the host device during subsequent access of the enciphered data will most likely be different than the bus that was previously used to encrypt the enciphered data and therefore the host device will not be able to properly decrypt the enciphered data. Such protection from "replay attack" cannot be achieved by following the teachings of IBM. Therefore, IBM fails to disclose every limitation of Claim 1.

As to independent Claim 11, Applicant submits that IBM does not disclose a storage device reading a key distribution data block from a storage medium; the storage device processing at least a portion of said key distribution data block using at least one device key to compute a media key; the storage device fetching a nonce generated by a number generator; the storage device combining said nonce with said media key using a one-way function to generate a bus key; the storage device encrypting data read from the storage medium using the bus key generated by the storage device; and the storage device transmitting the encrypted data over a data bus to a host device. Instead, IBM discloses generating a title key K_t using a random number generator, which is used to encrypt data before storing the data on a storage medium. Since the title key K_t of IBM is not used to encrypt data read from a storage medium before transmitting the encrypted data over a data bus to a host device, IBM fails to disclose every limitation of Claim 11.

With respect to independent Claim 18, Applicant submits that IBM does not disclose a storage device that processes a portion of a key distribution data block using a device key to compute a media key, and uses a one-way function to combine the media key with a nonce to produce a bus key. Additionally, Applicant submits that IBM fails to disclose a storage device that encrypts data accessed from a storage medium using a bus key (that is derived using a one-way function to combine a media key with a nonce) prior to transmitting the encrypted data via a data bus to a host device, as recited in Claim 18.

Accordingly, Applicant respectfully requests withdrawal of the rejection of the independent Claims 1, 11 and 18. Claims 2-4, 6-9, 12-17 and 21-26 are each respectively

dependent on independent Claims 1, 11 and 11. Therefore, the rejected dependent claims are not anticipated at least for the same reasons as their respective independent claims.

In the Office Action, the Examiner rejects Claim 1 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,289,102 issued to Ueda et al. (Ueda). Applicant respectfully traverses this rejection.

In making the rejection, the Examiner relies on figure 24 of Ueda, which shows a decoder authentication circuit in an optical disk drive. In response, Applicant notes that Ueda fails to disclose an encryption bus key that is derived based on [1] a portion of the key distribution data block, [2] a device key assigned to the encryption subsystem and [3] the nonce generated by the number generator, as recited in Claim 1. At least for this reason, Applicant submits that Ueda does not anticipate Claim 1 and requests withdrawal of this rejection.

IV. Claims Rejected Under 35 U.S.C. § 103

The Examiner rejects Claims 5, 10 and 20 under 35 U.S.C. §103(a) as being unpatentable over IBM in view of U.S. Patent No. 5,949,881 issued to Davis (Davis). Applicant respectfully traverses this rejection.

As Claims 5, 10 and 20 are dependent on independent Claims 1, and 18, the discussion above with regard to the independent claims and IBM applies here. Because IBM does not contain limitations recited in Applicant's independent claims as set forth above, and because Davis does not cure these deficiencies, the combination of IBM and Davis does not teach or suggest Applicant's dependent claims. Therefore, Claims 5, 10 and 20 are patentable over IBM in view of Davis.

Additionally, Claims 5 and 20 are independently nonobvious as none of the cited references disclose or suggest that data transmitted over a data bus is encrypted using the bus key derived based on the nonce such that if the data is recorded at the time of transmission, the recorded data is not subsequently playable by a decryption subsystem that does not have access to the same nonce used by the encryption subsystem to encrypt the data transmitted over the data bus, as recited by Applicant.

In making the rejection, the Examiner asserts that although IBM does not explicitly disclose the limitations recited in Claims 5 and 20, David teaches that data transmitted over a data bus is encrypted using the bus key derived based on the nonce such that if the data is

recorded at the time of transmission, the recorded data is not subsequently playable by a decryption subsystem that does not have access to the same nonce used by the encryption subsystem to encrypted the data transmitted over the data bus, citing column 3, lines 5-15 and 50-65 of David. However, the portions of David referred to by the Examiner in no way teach or suggest protecting data transmitted over a bus using a bus key that is derived based on a nonce so that the data recorded at the time of transmission is not subsequently playable by a decryption subsystem that does not have the same access to the same nonce used by the encryption subsystem to encrypt the data transmitted over the data bus. Rather, the portions of the David referred to by the Examiner merely teaches encrypting message that is passed from a cryptographic coprocessor to a system processor using a temporary session key to prevent "replay" of previous messages. This means that the temporary session key of David cannot be used to play or decipher previous messages. Thus, David does not disclose encrypting data transmitted over a data bus using a bus key that is derived based on a nonce such if the data transmitted over the bus is effective in resisting against "replay" attacks. Accordingly, Applicant respectfully requests withdrawal of the rejection of Claims 5 and 20.

CONCLUSION

In view of the foregoing, it is believed that all claims now pending patentably define the subject invention over the prior art of record and are in condition for allowance, and such action is earnestly solicited at the earliest possible date. If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 02-2666 for any additional fees required under 37 C.F.R. §§ 1.16 or 1.17, particularly, extension of time fees. If a telephone interview would expedite the prosecution of this Application, the Examiner is invited to contact the undersigned at (310) 207-3800.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN, LLP

Dated: April 29, 2004

By: _____
Walter T. Kim, Reg. No. 42,731

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California 90025
(310) 207-3800

CERTIFICATE OF MAILING:
I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail , with sufficient postage, in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on April 29, 2004

_____
Marilyn Bass April 29, 2004